

Baseline Cyber Security Program



**NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Information Management and
the Chief Information Officer**

THIS PAGE INTENTIONALLY LEFT BLANK

BASELINE CYBER SECURITY PROGRAM

1. **PURPOSE.**

The purpose of this Policy is to provide an integrated organization-wide Risk Management Approach (RMA), set forth by the Department of Energy (DOE), to improve and maintain an agile Cyber Security Program (CSP) to protect organizational operations and assets consistent with associated risks. This NNSA Policy (NAP) prescribes a CSP that employs a Risk Management Framework (RMF) that is:

- a. Based on the principles, responsibilities, processes, and requirements in NAP-21, *Transformational Governance and Oversight*; and
- b. Consistent with and incorporates National Institute of Standards and Technology (NIST), Committee on National Security Systems (CNSS), and DOE requirements and guidelines.

All CSP practices, procedures, and plans developed within NNSA must be consistent with and incorporate the requirements of this NAP.

2. **CANCELLATION.**

- a. This NAP replaces all chapters except for Chapter VII, Incident Management of NAP 14.1-C, *NNSA Baseline Cyber Security Program*, dated 05-02-08.
- b. This NAP replaces NAP 14.2-C, *NNSA Certification and Accreditation (C&A) Process for Information Systems*.
- c. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with directive requirements. Cancelled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the cancelled directives.

3. **APPLICABILITY.**

- a. This NAP applies to all NNSA entities, Federal and contractor, that collect, create, process, transmit, store, and disseminate information on automated information systems for NNSA.
- b. **Contractors.** Except for the equivalencies/exemptions in paragraph 3.c., the Contractor Requirements Document (CRD), Attachment A, sets forth requirements of this NAP that will apply to site/facility management contracts.
 - (1) The CRD, Attachment A, must be included in the management contracts for all sites/facilities that collect, create, process, transmit, store, and disseminate information on automated information systems for NNSA. Additionally,

management contracts must include DOE Acquisition Regulation (DEAR) clause 952.204-77, Computer Security.

- (2) NNSA elements must notify contracting officers of affected site/facility management contracts to incorporate the CRD, Attachment A, into those contracts.
- (3) Once notified, contracting officers are responsible for processing contract actions in accordance with their respective process and appropriately incorporating the CRD, Attachment A, into the affected contracts via the laws, regulations, and DOE directives clause of the contracts.
- (4) As stated in DEAR clause 970.5204-2, *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors that have this NAP incorporated into their contracts are responsible for compliance with this NAP. Affected site/facility management contractors are responsible for flowing down the requirements of this NAP to subcontracts at any tier, to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this NAP and only incur costs that would be incurred by a prudent person in the conduct of competitive business.

c. Equivalencies/Exemptions.

- (1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at Title 50 U.S.C. sections 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.
- (2) Exemption. This NAP does not apply to Sensitive Compartmented Information (SCI) information systems located at NNSA Sites. SCI systems must comply with Director, Central Intelligence Directives (DCIDS), or Intelligence Community Directives (ICDS) Security Policies. The DOE Office of Intelligence and Counterintelligence approves operation of these information systems.

4. BACKGROUND.

This NAP was developed using DOE O 205.1B, *Department of Energy Cyber Security Program*, dated 05-16-2011, as a baseline and is tailored to meet the mission requirements of NNSA. This NAP incorporates and requires a CSP consistent with the unified cyber security framework outlined in National policies, instructions, standards and guidelines

issued by the Committee on National Security Systems (CNSS) and the National Institute of Standards and Technology (NIST).

Through the implementation of the CSP requirements outlined in this policy, NNSA Program Offices and their associated field sites, including NNSA laboratories and plants, can effectively meet the Department's FISMA obligations. In addition, NNSA Program Offices and their associated field sites can ensure implementation of cost-effective security controls/investments, consistent with DOE/NNSA mission requirements that are in alignment with current threats.

5. REQUIREMENTS.

- a. NNSA information assets must be protected in a manner commensurate with mission importance, significance to national security, threat capability, known vulnerabilities and consequence of loss for the information it processes. NNSA elements must develop and maintain a comprehensive Cyber Security Risk Management Implementation Plan that meets the following requirements:
 - (1) The NNSA and its elements must establish, and utilize a RMF to maintain a cost effective and secure environment that enables the organization to meet its mission and business goals and objectives that:
 - (a) Sets forth a RMF aligned with NIST Special Publication 800-39, *Managing Information Security Risk Organization, Mission, and Information System View* and NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.
 - (b) Establishes roles, responsibilities, communication, and risk reporting structure. Attachment D provides a template for risk reporting.
 - (c) Establishes a risk strategy and risk tolerance threshold based on the criticality of organizational mission and business functions.
 - (d) Adequately protects DOE/NNSA information and information assets in a cost effective manner by managing information security risks, considering mission priorities, and allocating resources to the most efficient solutions necessary to reduce risk to acceptable levels. The RMF:
 - i. Takes into account the need to harmonize mission execution and performance with security needs, business, structure, and security requirements;
 - ii. Provides the flexibility to tailor and implement risk mitigation controls in light of local threats, acceptable risks, mission needs, and environmental and operational factors;

- iii. Actively evaluates, responds to, and mitigates changing threats and evolving situations to continuously manage risk to acceptable levels as defined in site risk management plans and the enterprise threat tolerance statement levels;
 - iv. Includes continuous monitoring of information security management controls. This includes continuous assessment of the overall, ongoing effectiveness of the approach to managing cyber risk;
 - v. Implements Federal Information Processing Standards (FIPS) 199 and FIPS 200 for unclassified systems and Committee on National Security Systems (CNSS) requirements for national security systems. See Attachment C for a table mapping DOE information to CNSS Potential Impact Levels; and
 - vi. Incorporates and uses NIST SP-800 series publications as guidance in the development of their Cyber Security Risk Management Implementation Plans.
- (2) NNSA elements must leverage existing and/or enterprise cyber security risk solutions unless the approach does not address the varying mission needs, encounters significant technical barriers, or is not cost effective for implementation.
- b. Cyber Security Program Documentation.
- (1) The NNSA Administrator shall establish and maintain a Risk Management Implementation Plan. This plan must be based upon requirements outlined in DOE O 205.1B. This NAP serves as the NNSA Risk Management Implementation Plan.
 - (2) Each NNSA site must document their RMF in the Site Risk Management Plan. This plan is a management-level document approved by the Site Office Manager (SOM) in coordination with the Site Senior Contractor Management that details the site RMF, missions, threats, policies, procedures, and practices specific to the Site Office and M&O Contractors. See Attachment B for the Risk Management Plan outline.
- c. Governance.
- (1) NNSA risk management is governed by leadership, management, and technical experts consisting of the NNSA Management Council, Enterprise Cyber Security Advisory Board (ECSAB) and Site Level Risk Management Councils (SRMC). Figure 1 illustrates the relationships, the functions and basic processes of the governance

bodies. The ECSAB and SRMCs will publish associated charters, define processes, and issue work plans.

- (2) The NNSA Management Council governs the Cyber Security Program. Per NAP-20, *NNSA Management Council*, the Council is a forum for discussions and decisions regarding NNSA policies, practices, and priorities. These include: activities and decisions associated with the Planning, Programming, Budgeting, and Evaluation (PPBE) system; Human Capital Programs; Acquisition Management; Information Technology policies and initiatives for each NNSA Federal element; coordination of NNSA responses to Federal and DOE taskings and directives. As such, this Council will perform risk management at the enterprise level.
- (3) The Enterprise Cyber Security Advisory Board (ECSAB) will be chartered by the NNSA Management Council and chaired by the NNSA Associate CIO for Policy and Governance. Other members include the Associate CIOs for Classified Operations, Unclassified Operations, and Resource Management; and two representatives from each site who can effectively communicate information management (IT and Cyber Security) and mission requirements. While sites are addressing inclusion of the requirements of this policy into their contracts, site Authorizing Officials will serve as representatives on the ECSAB for their respective sites. The ECSAB oversees, advises on, and provides:
 - (a) A common NNSA approach to determine and manage residual risk;
 - (b) Policy and technology issues relevant to Information Technology and Cyber Security;
 - (c) Consultation with and feedback to the NNSA CIO;
 - (d) Information sharing among the Nuclear Security Enterprise (NSE) site risk management councils and the NNSA CIO concerning risk management; and
 - (e) Discusses and determines the detailed approach and procedures for the NSE for implementing the system-level management, operational and technical controls, further defined in DOE 205.1B to supplement the requirements of this NAP such as Warning Banners, plan of action and milestones, and media use.
- (4) Each site will have a Site Risk Management Council (SRMC). These site-level councils manage information management risks at their respective sites. At sites with M&O contractors, council members are selected to represent the site office and M&O contractor. For Headquarters, council members are selected by the CISO.

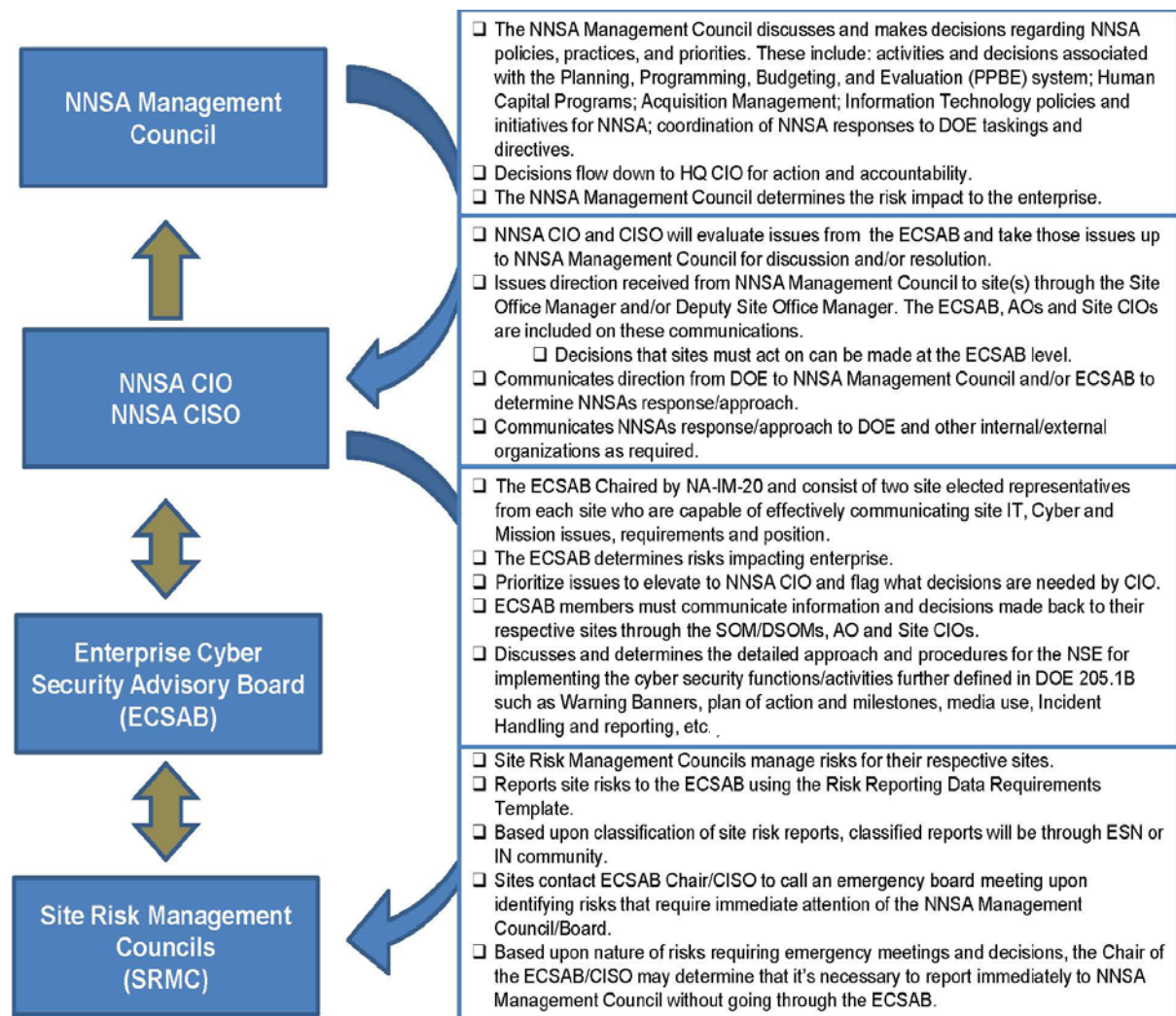


Figure 1 - Information Security Management Governance Communication Workflow

6. RESPONSIBILITIES.

a. Under Secretary for Nuclear Security/Administrator, National Nuclear Security Administration or designee.

- (1) Notifies contracting officers of which contracts are affected by requirements of this policy.
- (2) Retains overall responsibility and accountability for the CSP within the organization.
- (3) Serves as a member of the Department of Energy Information Management Governance Council. This authority may be further delegated within the organization.

- (4) Ensures the preparation and maintenance of organizational RMFs in the requirements section of this policy.
 - (5) Serves as the Authorizing Official (AO) for information systems within NNSA. This authority may be further delegated within the organization.
 - (6) Ensures that record management requirements are included throughout the CSP.
- b. NNSA General Counsel. Provides timely review and advice on all NNSA legal issues.
- c. NNSA Contracting Officers.
- (1) After notification by the appropriate program official, incorporate this NNSA Policy into affected contracts via the laws, regulations, and DOE Directives clauses of the contracts.
 - (2) Assist originators of procurement requests who want to incorporate this NNSA Policy in new non-site/facility management contracts, as appropriate.
- d. Associate Administrator for Defense Nuclear Security (NA-70).
- (1) As described in Public Law 106-65 dated October 5, 1999, the Chief, Defense Nuclear Security is responsible for the development and implementation of security programs for NNSA, including the protection, control and accounting of materials, and for the physical and cyber security for all facilities of the Administration.
 - (2) However, with regards to cyber security, NNSA Supplemental Directives NA-1 SD 226.1A, *Line Oversight and Contractor Assurance System*, and NA-1 SD 411.1-1C, *Safety Management Functions, Responsibilities and Authorities Manual*, established a functional line of authority for cyber security under the Associate Administrator for Information Management and Chief Information Officer (CIO), NA-IM, which delegates all cyber security program elements to NA-IM.
- e. Associate Administrator for Information Management and Chief Information Officer (CIO, NA-IM).

- (1) Supports the department-wide CSP as directed by the DOE Information Management Governance Council (IMGCC) by developing and maintaining NNSA's RMF, cyber security policies, procedures and threat statements.
 - (2) Provides direction to the NSE pertaining to risk management activities.
 - (3) Serves as a member of the DOE IMGCC and the NNSA Management Council.
 - (4) Is the "functional leader for cyber security" within the NNSA, as described in NA-1 SD 226.1A and NA-1 SD 411.1-1C.
 - (5) Conducts oversight activities of site office and Federal site's performance in the area of cyber security as described in NAP-21, NA-1 SD 226.1A, and NA-1 SD 411.1-1C.
 - (6) Ensures the integration of cyber security with capital planning and investment control, enterprise architecture, and acquisition/system development life cycles.
 - (7) Appoints the NNSA Chief Information Security Officer (CISO) with approval from the Administrator.
 - (8) Ensures that information systems are covered by approved security plans and are authorized to operate.
 - (9) Evaluates issues from the ECSAB and presents those issues to the NNSA Management Council for discussion and/or resolution.
 - (10) Notifies the ECSAB of performance and/or status of issues that are presented to the NNSA Management Council.
 - (11) Submits risk management tasks to SRMCs to include notifications to the Site Office based upon decisions of the NNSA Management Council.
- f. NNSA Chief Information Security Officer (CISO).
- (1) Serves as a member of the DOE Information Management Governance Council (IMGCC).
 - (2) Develops, maintains and manages an NNSA Enterprise CSP to fulfill NNSA's statutory and regulatory cyber security responsibilities.
 - (3) Ensures that security requirements specified in the Federal Information Security Management Act (FISMA) are accomplished in an efficient, cost-effective and timely manner.

- (4) Serves as the NNSA Cyber Security Risk Executive as described in NIST SP 800-39.
- (5) Ensures that the NNSA cyber security architecture supports and enables the NNSA's missions.
- (6) Oversees the development and implementation of an NNSA-wide cyber security incident reporting, assessment and response program.
- (7) Manages and provides the NNSA's response for all Agency-level cyber security inquiries (e.g., Congressional, Department of Homeland Security (DHS)), and cyber security program review requirements.
- (8) Serves as the primary point of contact for the CIO relative to cyber security activities with senior DOE management and other Federal Agencies.
- (9) Prepares and maintains an organizational RMF, to include a NNSA Risk Management Implementation Plan, which consists of site-level Risk Management Implementation Plans and other NNSA risk factors.
- (10) Ensures the allocation of sufficient resources to address enterprise cyber security risks.
- (11) Reviews quarterly/annual program assessment reports resulting from the continuous monitoring component of the RMF to complete the Information Surety Report or reporting to NA-1 and S-1.
- (12) Serves as the NNSA AO for Enterprise Systems as delegated by the Administrator.
- (13) Ensures the appointment of an ISSM to be responsible for developing and implementing the Risk Management Plan at the NNSA HQ Site and Enterprise.
- (14) Ensures policy and guidance established by the Department for Agency-wide telecommunications security programs to include Communications Security (COMSEC), TEMPEST, Protected Distribution Systems (PDS), and supporting transmission security programs are implemented.
- (15) Maintains communication between all elements concerning NNSA risk management activities.

- (16) Coordinates the sharing of threat information with Senior Department Managers, the Office of Intelligence and Counterintelligence, NNSA elements, and other U.S. Government officials.
 - (17) Designates one or more Authorizing Officials Designated Representatives (AODRs) to perform duties in accordance with NIST SP 800-37.
 - (18) Ensures personnel are sufficiently trained to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines.
 - (19) Issues guidance/direction in accordance with the requirements outlined in this policy.
- g. Enterprise, Federal Site, and Site Office Manager / Site AO.
- (1) Serves as the AO responsible for Federal oversight of M&O site cyber security programs and systems under their purview as delegated by the Administrator. The SOM may further designate other AOs for their respective site. The SOM may also appoint AODRs.
 - (2) Completes Federal/Enterprise AO functions consistent with FISMA, NAP-21, *Transformational Governance and Oversight*, and risk management guidance available from DOE and NNSA governance structures.
 - (3) Participates with the Senior Site Contractor Management (i.e., Laboratory Director, Plant Manager), and applicable mission owner(s) approving acceptable risk and processes the site specific RMF and places it into the M&O contract.
 - (4) Ensures the development of and approves the site Risk Management Plan.
 - (5) Ensures external systems and services provided by M&O/Support Contractors meet acceptable risk levels.
 - (6) Ensures implementation of the RMF, as prescribed in NIST SP 800-37, is in individual system security plans, and implementation of continuous monitoring plans. This also includes expanding the RMF at the site level to include the site specific interfaces.
 - (7) In conjunction with the Senior Site Contractor Management and mission owners, appoints two representative(s) to participate on the ECSAB.

- (8) Supports the CISO by providing a representative(s) to support the NNSA Cyber Security Risk Executive when requested.
 - (9) In conjunction with the Senior Site Contractor Management and mission owners, appoints members of SRMC. Sites that fall under the purview of HQ will coordinate with CISO on appointment of council members.
- h. Authorizing Official Designated Representative (AODR).
- (1) Acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process.
 - (2) Can be empowered by authorizing officials to make certain decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk.
 - (3) May also be called upon to prepare the final security authorization package, obtain the authorizing official's signature on the security authorization decision document, and transmit the security authorization package to appropriate organizational officials.
 - (4) Advise SOM and Laboratory Director/Plant Manager if RMF risk parameters are exceeded or might be exceeded.
 - (5) Note: The only activity that cannot be delegated to the designated representative by the authorizing official is the security authorization decision and signing of the associated security authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation).
- i. Information Security Site Manager (ISSM).
- (1) Develops, implements, and monitors the Federal element's CSP in accordance with Site Risk Management Plan and Program Execution Guidance (PEG).
 - (2) Maintains record copies of CSP Plans and reports to include Information Systems Security Plans (ISSPs) for systems under their cognizance.
 - (3) Ensures written appointments of ISSOs for information systems and ensures site personnel are aware of and fulfill their information security

management/user duties as described in the Site Risk Management Plan.

- j. The Enterprise Cyber Security Advisory Board (ECSAB).
 - (1) Determines if a risk impacts a site or the Enterprise.
 - (2) Provides independent consultation and feedback from the NNSA elements and Headquarters site perspective to the NNSA CIO.
 - (3) Develops a common NNSA approach to determine and manage residual risk and report results to the NNSA CIO.
 - (4) Advises and coordinates policy and technology issues relevant to Information Technology and Cyber Security and report results to the NNSA CIO.
 - (5) Prioritizes issues to elevate to the NNSA CIO, and flagging decisions needed from the NNSA CIO/Management Council.
 - (6) Promotes cooperation, collaboration, and information sharing among the NNSA sites concerning risk management activities to include shared responsibilities for joint/leveraged authorizations and services provided by external providers.
 - (7) Communicates information and decisions made back to sites and appropriate Authorizing Officials.
- k. Site Risk Management Councils (SRMC).
 - (1) Submit insufficiently mitigated risks and other issues to the ECSAB.
 - (2) Notify AOs regarding communications to the ECSAB information/decision from the NNSA CIO.

7. REFERENCES.

- a. Federal Laws and Regulations
 - (1) P.L. 106-65, National Defense Authorization Act [Section 3212(d)], enacted October 1999.
 - (2) P.L. 107 347, Title III, Federal Information Security Management Act of 2002 (FISMA), enacted December 2002.
- b. Office of Management and Budget (OMB) Circulars. Located At http://www.whitehouse.gov/omb/circulars_default/.

- c. OMB Memoranda Pertaining to Information Technology Security and Management. Located at http://www.whitehouse.gov/omb/memoranda_default/.
- d. DOE Orders, Manuals, Notices, and Guidelines. Located at <https://www.directives.doe.gov/directives>.
 - (1) Deputy Secretary's Memorandum titled *Cyber Security Management*, dated 12-7-09.
 - (2) DOE O 471.6, *Information Security*, dated 6-20-11.
 - (3) DOE O 205.1B, *DOE Cyber Security Program*, dated 5-16-11.
- e. NNSA Policies
 - (1) NAP 70-.4, *Information Security*, dated 7-2-10.
 - (2) NAP 21, *Transformational Governance and Oversight*, dated 2-28-11.
 - (3) NAP 20, *NNSA Management Council*, dated 8-31-07.
 - (4) NA-1 SD 411.1-1C, *NNSA Safety Management Functions, Responsibilities and Authorities Manual (FRAM)*, dated 2-15-08.
 - (5) NA-1 M 226.1A, *NNSA Line Oversight and Contractor Assurance System (LOCAS)*, dated 10-17-08.
- f. Other
 - (1) 32 CFR 2001.23, *Classification Marking in the Electronic Environment*, dated 7-01-10.
 - (2) 32 CFR 2001.24, *Classified National Security Information-Additional information*, dated 6-28-10.
 - (3) Atomic Energy Act of 1954, as amended.
 - (4) E.O. 12344, *Naval Nuclear Propulsion Program*, dated 2-1-82.
 - (5) E.O. 13526, *Classified National Security Information* dated 1-5-10.
 - (6) NSPD-28, *United States Nuclear Weapons Command and Control, Safety, and Security*, dated 6-20-03.
 - (7) National Security Agency/Central Security Service, *Storage Device Declassification Manual (SDDM)*, dated 12-07.

- (8) Issuances of the Committee on National Security Systems (CNSS). Index of National Security Systems' Issuances can be found at www.cnss.gov/Assets/pdf/CNSS-INDEX.pdf.
- (9) National Institute of Standards and Technology (NIST) Standards and Guidelines. Directory of NIST Standards and Guidelines can be found at <http://csrc.nist.gov/index.html>.

8. DEFINITIONS.

- a. **Contractor Assurance System (CAS)** – Requirements for a contractor assurance system are described in DOE O 226.1A, *Implementation of Department of Energy Oversight Policy*, Attachment 1, Appendix A "Contractor Assurance Systems."
- b. **Cyber Security** – The management, technical, and operations controls and risk management process used to mitigate cyber risk for providing the required and appropriate level of confidentiality, integrity, and, availability and accountability for of DOE/NNSA information stored, processed, or transmitted on electronic systems and/or networks.
- c. **Enterprise System** – Systems within NNSA where the accreditation boundary covers multiple sites and multiple local Authorization Official Jurisdictions.
- d. **Authorizing Official (AO)** – A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the Nation. The AO typically have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system. Through the security authorization process, AOs are accountable for the security risks associated with information system operations. Accordingly, AOs are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Authorization Officials also approve security plans, memorandums of agreement or understanding, plans of action and milestones (POA&Ms), and determine whether significant changes in the information systems or environments of operation require reauthorization. The AO can deny authorization to operate an information system or if the system is operational, halt operations, if unacceptable risks exist. The AO coordinate their activities with the risk executive (function), CIO, CISO, common control providers, information system owners, Information ISSO, security control assessors, and other interested parties during the security authorization process. With the increasing complexity of mission/business processes, partnership arrangements, and the use of external/shared services, it is possible that a particular information system may involve multiple AOs. If so, agreements are established among the authorizing officials and documented in the security plan. Authorizing Officials are responsible for ensuring that all activities and functions associated with security authorization that are delegated to AODRs are carried out. The role of AO has inherent U.S.

Government authority and is assigned to government personnel only.

9. CONTACT. Questions concerning this NNSA Policy should be addressed to the Office of the Associate Administrator for Information Management and Chief Information Officer at (202) 586-9728.

BY ORDER OF THE ADMINISTRATOR:



Thomas P. D'Agostino
Administrator

Attachments:

- A: Contractor Requirements Document
- B: An Example of a Site Cyber Security Risk Management Plan
- C: Table Mapping DOE Information Groups to CNSS 1253 Potential Impact Levels
- D: Risk Reporting Data Requirements Template

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT A CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the requirements for National Nuclear Security Administration (NNSA) contractors with access to NNSA and Department of Energy (DOE) information systems. Contractors must comply with the requirements listed in the CRD.

Regardless of the performer of the work, the contractor is responsible for complying with and flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

The contractor will ensure that it and its subcontractors cost-effectively comply with the requirements of this CRD. The Contractor must:

1. Ensure assets are protected in a manner commensurate with mission importance, significance to national security, threat, vulnerability and magnitude of harm relative to compromise.
2. Develop and maintain a comprehensive Cyber Security Program (CSP) that meets the following requirements:
 - a. Must establish, and utilize a Risk Management Framework (RMF) in a manner that maintains a cost effective and secure environment to enable the organization to meet its mission and business goals and objectives that:
 - (1) Sets forth a RMF aligned with NIST Special Publication 800-39, *Managing Information Security Risk Organization, Mission, and Information System View* and National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.
 - (2) Establishes roles, responsibilities, communication, and risk reporting structures.
 - (3) Establishes a risk strategy and risk tolerance threshold based on the criticality of organizational mission and business functions.
 - (4) Adequately protects DOE/NNSA information and information assets in a cost effective manner by managing cyber security risks considering mission priorities and allocating resources to the most efficient solutions necessary to reduce risk to acceptable levels. The RMF:

- i. Takes into account the need to harmonize mission execution and performance with security needs, business, structure, and security requirements.
 - ii. Provides the flexibility to tailor and implement security programs in light of local threats, acceptable risks, mission needs, and environmental and operational factors
 - iii. Actively evaluates, responds to, and mitigates changing threats and evolving situations to continuously manage risk to acceptable levels as defined in site risk management plans and the enterprise threat tolerance statement levels.
 - iv. Includes continuous monitoring of information security management controls. This includes continuous assessment of the overall, ongoing effectiveness of the approach to managing cyber risk.
 - v. Implements Federal Information Processing Standards (FIPS) 199 and FIPS 200 for unclassified systems and Committee on National Security Systems (CNSS) requirements for national security systems.
 - vi. Incorporates and uses all NIST SP-800 series publications as guidance in the development of their RMF.
 - vii. Leverages existing and/or enterprise cyber security risk solutions unless the approach does not address the varying mission needs, encounters significant technical barriers, or is not cost effective for implementation.
 - b. Ensures the implementation of a framework for the Planning, Programming, Budgeting, and Evaluation (PPBE) process and allocation of resources with the cyber security program.
3. Cyber Security Program Assurance
 - a. In the context of M&O Contractors, the approach adopts and utilizes the flexibility and tailoring described above and includes focus on Federal oversight of high-level balanced outcomes and outputs of the Contractor Assurance Systems (CAS), and the contractor's performance in meeting cyber security expectations as defined in NAP-21, *Transformational Governance and Oversight*.
 - b. Contractor Assurance Systems must provide quarterly CSP and performance reporting in accordance with direction from the NNSA CISO covering the following elements:

- (1) Site Cyber Security Program Performance
 - (2) Site Cyber Security Budget
4. Cyber Security RMF Documentation
- a. Each NNSA site must document their RMF in the Site Risk Management Plan. This plan is a management-level document approved by the Site Office Manager (SOM) and the Senior Site Contractor Management (i.e., Laboratory Director, Plant Manager) that details the site RMF, missions, threats, policies, procedures, and practices specific to the Site Office and M&O Contractors. See Attachment B for an example of a risk management plan outline.
5. Roles and Responsibilities
- a. Senior Site Contractor Management
 - (1) Leads the process in conjunction with the site office manager and the mission owners to set an acceptable risk level for those information assets under their purview in a Site Risk Management Plan.
 - (2) Ensures Laboratory or Plant develop and maintain a comprehensive CSP employing an RMF based on the acceptable risk level identified in the Site Risk Management Plan.
 - (3) Ensures Laboratory or Plant develop a Contractor Assurance System based on the requirements outlined in NAP-21, NNSA Supplemental Directive NA-1 M 226.1A, *NNSA Line Oversight and Contractor Assurance System (LOCAS)*, and the requirements of this policy.
 - (4) In conjunction with the site office manager and the mission owners, appoints representative(s) to participate on the Enterprise Cyber Security Advisory Board (ECSAB).
 - b. M&O Chief Information Officer
 - (1) Assists the Senior Contractor Official with developing and maintaining a comprehensive CSP program including site management roles and responsibilities, developing a RMF, and Contractor Assurance System.
 - (2) Assumes full accountability for site execution of an effective CSP.
 - (3) Assumes the operation of systems in accordance with the site's approved risk management plan. Makes risk management recommendations to the Senior Contractor Official and manages the implementation of the site CSP.

- (4) Ensures the appointment of an ISSM to be responsible for direct oversight of development and implementing the CSP at the M&O site.
- c. Contractor Information Security Site Manager (ISSM)
- (1) Develops, implements, and monitors the M&O CSP in accordance with Site Risk Management Plan and Program Execution Guidance (PEG).
 - (2) Maintains record copies of the M&O's CSP Plans and reports to include Information Systems Security Plans (ISSPs) for systems under their cognizance.
 - (3) Ensures written appointments of ISSOs for information systems operated by their respective NNSA M&O and site personnel are aware of and fulfills their cyber security management/user duties as prescribed by the RMF documented in the Site Risk Management Plan.

ATTACHMENT B
OUTLINE FOR THE SITE CYBER SECURITY RISK MANAGEMENT PLAN

- 1) Chapter 1 – Overview of the Cyber Security Program
 - 1.1 Risk Management Framework (RMF) - Provide an RMF in a manner appropriate to meet requirements outlined in this NAP, 14.1-D.
 - 1.2 Implementation of Federal Requirements, Standards and Guidelines
 - 1.3 Roles and Responsibilities/Federal Governance Model
 - 1.4 Formal Information Systems Authorization Process (i.e. certification and accreditation)
 - 1.4.1 Information System Security Plans (ISSPs)
 - 1.4.2 Management, Operations, and Technical Controls
 - 1.5 Performance Metrics, Assessments, and Oversight Activities
- 2) Chapter 2 – Program Plan of Action and Milestones for execution of site RMA.
- 3) Chapter 3 – Implementation Status
 - 3.1 Completed Actions - Actions that have already been completed under NNSA Memorandum, Deviation Approval to Use Federal Cyber Security Standards and Guidance in lieu of NNSA Policy Letter 14.1-C & 14.2-C dated May 24, 2010.
 - 3.2 Plans and Milestones for Completing Remaining Actions - Describe Plan of Actions that still need to be executed as part of the implementation of the NNSA OCIO Cyber Security Program.

THIS PAGE INTENTIONALLY LEFT BLANK

**ATTACHMENT C
TABLE MAPPING DOE INFORMATION GROUPS TO CNSS 1253 POTENTIAL
IMPACT LEVELS**

Table 1-Mapping DOE Information Groups to CNSS 1253 Potential Impact Levels

DOE Information Group [1]			CNSSI 1253 Potential Impact for Loss of Confidentiality
Confidential (NSI)			Low
Confidential RD[2]			Moderate
Confidential RD [4]	Sigma	1,2,3,4,5,9,10,11,12, and 13	Moderate
Secret (NSI)			Moderate
Secret RD			Moderate
Secret RD [3]	Sigma	15, 18and 20	Moderate to High
Secret RD [3]	Sigma	14	High
Top Secret (NSI) Top Secret RD		14, 15 18 and 20	High

[1] Potential levels of impact for Integrity and Availability are determined by use of the data as specified by the Information and Information System Owner as part of the Information System Categorization process of CNSSI 1253.

[2] Restricted Data (RD) restrictions described in the Atomic Energy Act of 1954 (as amended) are additional “need to know” access protections, but not additional consequences from authorized disclosure. Unlike NSI, RD category also has no automatic “declassify on date (or event)” as does NSI.

[3] Secret RD, Secret RD with Sigmas, and Top Secret NSI and RD start at the highest CNSSI 1253 potential impact for loss of confidentiality. The initial system categorization level may be adjusted using the site RMF in accordance with Paragraph 2.1.3 of CNSSI 1253.

[4] Refer to DOE O 452.8, *Control of Nuclear Weapon Data* for handling unmodified legacy Nuclear Weapon Data.

NOTE: For additional direction on authorization/control requirements for the RD category, see DOE O 452.7, *Protection of Use Control Vulnerabilities and Design*, DOE O 452.8, *Control of Nuclear Weapon Data*, and DOE O 457.1, *Nuclear Counterterrorism*.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT D
RISK REPORTING DATA REQUIREMENTS TEMPLATE

Classification Level: _____

Location:	
Background:	
General Discussion:	
PRIORITY:	Emergency: _____ Urgent: _____ Routine: _____ Date Required: ____ / ____ / ____
Summary of Risk Information: (Description, Impact, Category, Scope, and Likelihood)	
Risk Management Advisory Board Recommended Action:	
Affected Sites:	
Affected Systems:	
Cost Mitigation:	

Classification Level: _____